

Year 2000

Supplier Capability
Assessment Guide

Prepared by:

***DEFENSE LOGISTICS AGENCY
SUPPLIER CAPABILITY ASSESSMENT TEAM***

February 3, 1999

Table of Contents

Sections:

- i. DoD Letter to Suppliers on Y2K
- I. Preface – How to use this “Toolkit”
- II. Introduction -- The Y2K Problem
- III. Overview of the Y2K Supplier Capability Assessment Process
- IV. Y2K Supplier Capability Assessment Checklist
- V. Tutorial on Y2K and Business Operations
- VI. Y2K Case Studies – What Suppliers are Doing
- VII. Y2K Disclosure by Publicly Held Companies
- VIII. Information Sources/Web Sites
- IX. Points of Contact

Send questions or suggestions for improving this toolkit to Mr. David Robertson,
DCMC Paperless Team, (703) 767-3351, DSN 427-3351, or Internet
david_robertson@hq.dla.mil.

DoD Letter to Mission Critical Suppliers

The DCMC Commander, on behalf of the Military Services and Defense Agencies, sent the following letter to all critical defense suppliers scheduled to receive a Y2K assessment. The purpose of the letter is to increase supplier awareness of the possible impact of Y2K on their business and manufacturing processes. Field offices should refer to this letter during their initial discussions with supplier management.

Although the letter did not specifically request a response, many suppliers are voluntarily providing information to Headquarters DCMC on their Y2K efforts.

- All supplier responses will be forwarded to the appropriate CAO.
- When conducting the assessment:
 - Let the supplier know you have reviewed their response.
 - Only ask about areas that are *not* addressed in the supplier's response, or need clarification.

Section I

Preface – How To Use This “Toolkit”

This toolkit was developed by the Defense Logistics Agency (DLA) Supplier Capability Assessment Team to help field offices assess the Year 2000 (Y2K) readiness of those contractors who supply our most critical defense items. In preparing the toolkit, we interviewed industry and government experts, reviewed publications, and browsed web-sites for information on the impact of Y2K on day-to-day operations. The resulting toolkit provides field offices with essential information for conducting a thorough assessment of critical. Here are some tips on getting the most from the toolkit.

- Prepare for the assessment
 - Review the toolkit paying particular attention to:
 - Section II, Introduction – The Y2K Problem.
 - Section III, Overview of the Y2K Assessment Process.
 - Section IV, Y2K Supplier Capability Assessment Checklist.
 - Section V, Tutorial on Y2K and Business Operations.
 - Review the supplier assignment list in the database provided as Attachment 1 of the DCMC Tasking Memo.
 - Identify the assessment categories assigned to your suppliers (DCMC field offices will do assessments at “High” and “Moderate” category suppliers).
 - Schedule assessments.
- Do the assessment
 - Use the DoD Letter to Suppliers to initiate discussion and emphasize the importance of this effort.
 - Conduct the assessment using the checklist and drill-down questions provided in Section IV as a guide. From your assessment, determine the Y2K impact on the supplier and the status of their efforts to address the problem.
- Report assessment results using the database provided with the DCMC Tasking Memo. The database contains basic contractor information (i.e., name, CAGE Code, CAO, etc.).

Field offices play a vital role in evaluating Y2K status. This is especially critical at locations where Y2K-related failures would significantly disrupt support to the warfighter. As field office personnel, you are in the best position to evaluate the effectiveness of supplier efforts -- your contribution is essential!

Section II

Introduction -- The Y2K Problem

The Y2K problem is caused by a "shortcut" used in many computers and microchips. In the past, to conserve memory, programmers used two numbers to record the year – for example, 72 would mean 1972. These manufacturers have made considerable efforts since 1995 to ensure their products are capable of accurately recognizing and manipulating dates beyond 1999¹. However, older systems and equipment is still vulnerable and may, on January 1, 2000, recognize 00 not as 2000 but as 1900, 1980, or some other date.

Hardware and Software manufactured before 1997 poses significant risk of having Y2K compliance problems and should be evaluated. Electronic Commerce Resource Center Study 1998.

This could cause them to either shut down or generate incorrect data. At companies that depend on automated systems for such functions as tracking parts, paying employees, controlling machines, or running tests, that could be a big problem.

To date, Y2K remediation efforts have focused on computer-based business systems and information technology products. However, many companies currently addressing Y2K problems in computer systems may be overlooking potential problems embedded in their manufacturing and management systems. Modern manufacturing and management systems rely heavily on date processing and date-sensitive equipment to perform numerous, essential functions. As a result, the Y2K problem potentially impacts every piece of hardware that contains a microchip including:

- manufacturing control systems
- telecommunications
- gas, water, and electrical utilities
- environmental control systems (e.g., HVAC)
- Safety and security (e.g., fire sprinklers, alarms)

Nearly 50% of PCs shipped in early '97 still failed Year 2000 rollover testing. Greenwich Mean Time Study 1997

An estimated 50 million devices out of 25 billion embedded in automated systems are not Y2K compliant. Gartner Group Study 1997

¹ Harris N. Miller, President, Information Technology Association of America. The Impact of the Year 2000 Date Change Situation on PC Users. Testimony before the House Government Reform and Oversight Committee, September 10, 1996.

Additionally, there are indications that many small and medium-sized businesses may be lagging in their efforts to minimize Y2K-related disruptions of their business processes. While the "fix" is straightforward, many systems and interfaces are complex, which makes repair and replacement work time consuming. Thus, Y2K is primarily a management problem.

As of 1997, 88% of all companies with fewer than 2000 employees had not started Year 2000 remediation projects. Gartner Group Study 1997

An estimated 40% of vendors have not started Y2K remediation projects. Electronic Commerce Resource Center 1998

A detailed discussion of the Y2K "fix" is provided in the pamphlet, Small Business and the Year 2000: Are You Ready to do Business in the Year 2000, published by the Manufacturing Extension Partnership (MEP) (See Section V). The pamphlet is available at <http://www.mep.nist.gov> (click on "Y2K MFG Hot Topics" icon). A hyperlink to the pamphlet is at the bottom of the MEP Hot Topics page).

The pamphlet provides an informative, easy to understand information on the Y2K problem. It will give field personnel the necessary background information for doing the assessments. The pamphlet identifies five key steps contractors should be undertaking to assure they are ready for Y2K.

Awareness – *begin by educating and involving all levels of the company in solving the Y2K problem. This includes having top-management support and commitment (e.g., personnel, material, money, etc.) to make sure the company is ready for Y2K.*

Inventory – *companies should identify and rank (by how critical it is to the company's business) all computer-based systems, components, service providers, and hardware containing microchips that support their business. Including:*

- *Company-furnished*
- *Employee-furnished*
- *Prime Contractor/Trading Partner-furnished*
- *Government-furnished*

Assessment -- *starting with the most critical items on the inventory, companies need to determine which systems are date sensitive and whether they will fail when the century changes. Once the company has determined the state of readiness for each system and component listed in their inventory, they should develop one of three possible remediation strategies for those systems that need to be fixed.*

- *Repair the system*
- *Replace the system*
- *Retire the system*

If the company decides to repair a system, there are two possible approaches:

- *Date expansion – the ability to process century as well as 2-digit year*
- *Windowing – inserting logic in the system to recognize 00 as 2000*

Most companies are taking a mixed approach, fixing some systems using windowing logic and others with date expansion.

Correcting and Testing – *the best way to determine whether a system is ready for Y2K is to test the system as if it were already the year 2000. Testing verifies that the repaired or replaced system operates properly when the date changes and that existing business functions (such as accounting, inventory control, and order tracking) continue to operate as expected. There are several critical tests companies should perform once they have changed or replaced a system.*

- *Can the system operate correctly after the date has rolled over from 12/31/1999 to 1/1/2000?*
- *Because the year is a leap year, will the system recognize 2/29/2000 as a valid date and that it will roll over from 2/28/2000 to 2/29/2000 and from 2/29/2000 to 3/1/2000?*
- *Can the system “look back” -- will the system recognize data from some period before 1/1/2000 after the date has rolled over from 12/31/1999 to 1/1/2000?*

Implementation – *before companies install replacement or repaired systems, they should develop installation and contingency plans. The installation plan may include testing in production to ensure the installed systems are working as expected.*

Obviously, continued supplier performance in the Year 2000 is critical to our nation's defense. In order to promote continued performance and mitigate the risks of non-performance, the Joint DoD Supplier Capability Working Group (JSCWG) developed this “toolkit” to assess the Y2K efforts at supplier locations where a Y2K-related failure would significantly disrupt support to the warfighter.

- The evaluation uses standard “checklist” approach.
- Every effort will be made to use existing information on suppliers' Y2K status instead of on-site evaluations (Securities and Exchange Commission disclosures, supplier web sites, industry association data, etc.).
- Only the most critical suppliers -- where Y2K status information is not available -- will be subject to an on-site review.

Based on the results of your assessments, DoD will determine the risk of non-compliant suppliers and develop mitigation plans to ensure uninterrupted support to the warfighter.

Section III

Overview of the Y2K Supplier Capability Assessment Process

Supplier readiness is being assessed in six steps.

1. **Identify critical items.** The Military Services and DLSC have consulted with subject matter experts and screened their logistics support databases to determine which support items are the most critical.
2. **Identify critical suppliers.** Critical suppliers have been identified by matching the critical NSN to the suppliers' Commercial and Government Entity (CAGE) code and to the Original Equipment Manufacturer (OEM) CAGE code.
3. **Assigning assessment categories.**
 - Suppliers have been assigned to assessment categories by the Services and DLA based on volume of sales, number of critical items provided, and the following characteristics:
 - Sole and limited sources,
 - Direct Vendor Delivery/Prime Vendor (DVD/PV) arrangements,
 - Business size,
 - OEM coding,
 - Long procurement lead-time of record, and
 - Industrial capability support.Exhibit 1 shows the Military Service and DLA ranking strategies for assigning assessment categories.
 - The Military Services and DLA critical supplier lists have been combined to provide a consolidated list of DoD critical suppliers for Y2K assessment. Exhibit 2 shows the process for consolidating and developing the final Prioritized Suppliers List provided in Section X.
4. **Assess suppliers' Y2K compliance.**
 - JSCWG must obtain certain information on supplier Y2K remediation efforts. To do this in the most practical and unobtrusive manner, the JSCWG developed the assessment process flow shown in Exhibit 3.
 - Where possible, supplier Y2K status has been ascertained using reliable information available through industry associations, Securities and Exchange Commission (SEC) disclosures, supplier Web-sites, etc.

Guidance and web-sites for obtaining information on contractor Y2K status is included in Sections VIII and IX.

- Suppliers have been assigned to a field office for assessment when reliable information on a supplier's Y2K status *is not* available.
- Various methods, keyed to the supplier's assessment category, will be used to conduct assessments. Exhibit 4 shows the assessment categories and the associated supplier assessment tools.

DCMC field offices will assess suppliers in the "High" and "Moderate" assessment categories only if reliable information on the supplier's Y2K status is not available and the supplier is assigned to DCMC for contract administration.

- The checklist included in Section III has been developed to for use during all assessments. The provides summary level and drill-down questions to address:
 - Has the supplier assessed the impact of Y2K?
 - Are products/services affected?
 - Is the supplier already Y2K ready?
 - If not, has the supplier developed adequate plans?
 - When does the supplier expect to become Y2K ready?
 - Does Y2K remediation impact financial stability?
 - What contingency plans have been developed?
 - Is a follow-up recommended?
 - To provide sufficient opportunity to mitigate the risk of disruption, these assessments must be completed by mid-April 1999. Exhibit 5 shows the assessment timeline.
5. **Provide assessment results.** Assessment results will be reported to the HQ DCMC and forwarded to the Joint Supplier Capability Working Group. Guidance on how and when to report is provided in Attachment 1 and 2 of the DCMC Tasking Memo.
6. **Prepare contingency plans.** If the assessment results indicate a supplier is at risk, the Military Service and Defense Agency buying offices will be tasked to develop contingency plans to ensure continued support to the warfighter.

Exhibit 1 -- MILSVCs/DLA Ranking Strategy

CATEGORY	USA	USAF	USN	USMC	DLA
Very High	• Safety	• Prime Vendor (IMM Determined Critical)	• None	• IMM Determined Critical	• Prime Vendor
High	• Sole Source	• Sole Source for 5 or More Items	• IMEC 5/4 NMCS and 4CAT IV • SSPO Items • NRP Items	• Sole Source for 6 or More Items	• Sole Source for 5 or More Items
Moderate	• Long PLT	• Sole Source for 1-4 Items	• IMEC 4 PMCS and 4 CAT III	• Sole Source for 1-5 Items	• Sole Source for 1-4 Items • DVD Supplier
Low	• DVD	• None	• None	• None	• Long PLT Item Supplier (Not Sole Source or DVD)
Very Low	• Any Remaining	• None	• None	• None	• Not Sole Source, DVD, or Long PLT Item Supplier

*IMM - Integrated Material Manager

Exhibit 2 -- Prioritized Suppliers

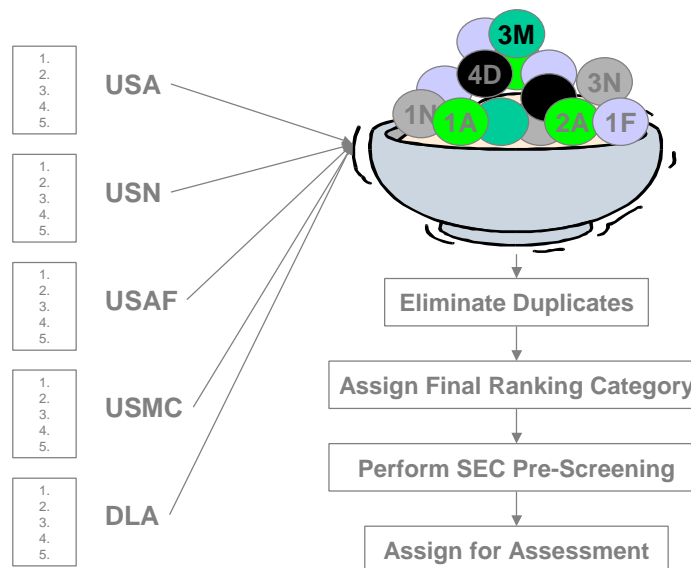


Exhibit 3 -- Assessment Process Flow

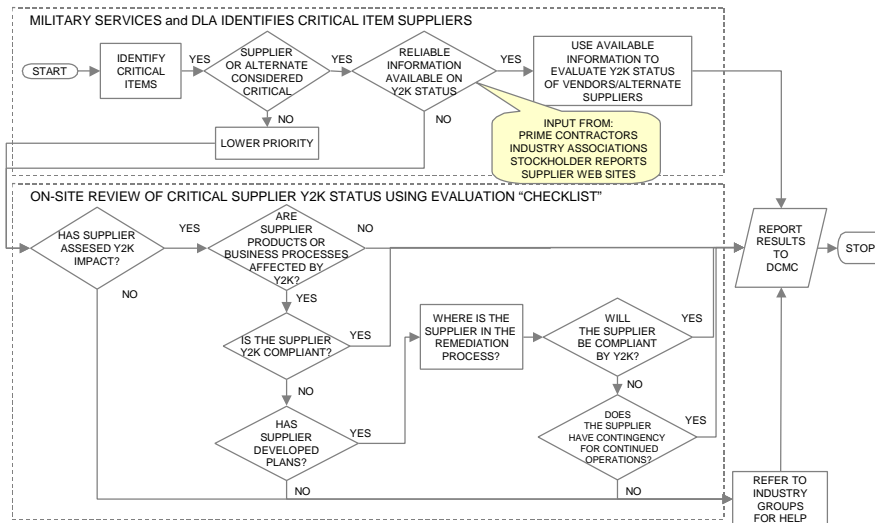
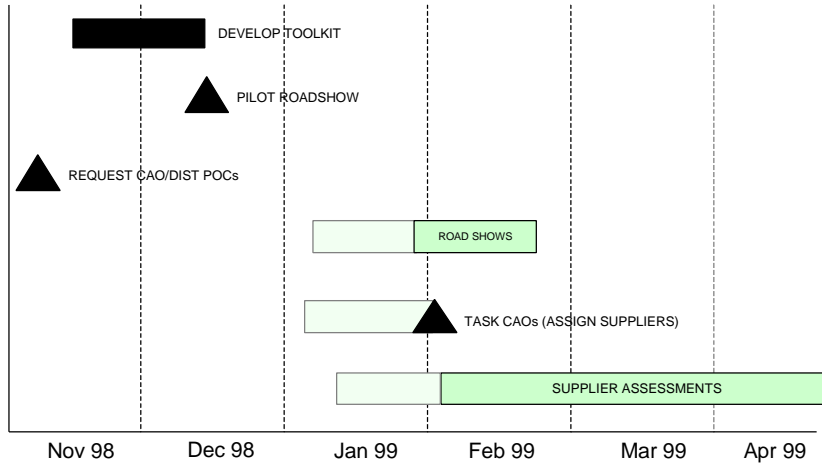


Exhibit 4 -- Assessment Categories

Assessment CATEGORY	SUPPLIER ASSESSMENT TOOLS	WORKLOAD ESTIMATE	OPR
Very High	<ul style="list-style-type: none"> Examination/Testing Discuss Financial Impact 	A Time Machine! Days/Weeks/TDY	IMM
High	<ul style="list-style-type: none"> Site Visits/Detailed Discussion w/Management and Key Personnel Review of Test Results/Supporting Documents Evaluation of Contingency Plans Discuss Financial Impact Review SEC Disclosure (if available/adequate) 	"Show me what you've done and what you plan to do..." 3-6 hours +TDY	DCMC CAO
Moderate	<ul style="list-style-type: none"> High Level Discussion w/Management and Key Personnel (On-Site or Telephone) Review SEC Disclosure (if available/adequate) 	"Give me some details..." 1-3 hours +TDY	DCMC CAO
Low	<ul style="list-style-type: none"> Discussions w/Management (Telephone) Review SEC Disclosure (if available/adequate) 	"Tell me what you've done..." 1 hour	IMM
Very Low	<ul style="list-style-type: none"> Minimal Inquiry Review Available Information Review SEC Disclosure (if available/adequate) 	"Tell me about your Y2K status" .5 hour	IMM

*IMM - Integrated Material Manager

Exhibit 5 -- Assessment Timeline



Y2K Supplier Capability Assessment Checklist

Introduction.

In order for DoD to work effectively toward a solution, the JSCWG must obtain certain information on supplier Y2K remediation efforts. To do this in the most practical and unobtrusive manner, the JSCWG intends to rely heavily on information that is already available through industry associations, non-profit EC/Y2K organizations, and the President's Council on Y2K Conversion. Guidance on how to obtain information on contractor Y2K status is included in Sections VIII and IX.

Additionally, prime contractors or other government activities have already reviewed many suppliers. If so, ask the supplier to provide a copy of the review results along with a point of contact at the reviewing activity for verification. If the information provided is credible and provides sufficient information regarding the supplier's Y2K readiness, an additional assessment may not be required. The decision whether an additional assessment is required rests with the field office.

If information on critical item contractors' Y2K preparedness is unavailable through these sources, an assessment should be conducted using the enclosed Y2K Supplier Capability Assessment Checklist. The checklist's high-level questions provide a quick rating of a contractor's chance of success in completing Y2K projects in time to prevent the disruption of essential business functions.

The depth of risk assessment interview shall be consistent with the degree of risk. For example:

- In the "Very Low" category a minimal inquiry using available information or brief telephone discussions is sufficient.
- In the "Low" category, the checklist should be completed during a telephone interview, accepting the contractor's statements at face value.
- For the "Moderate" category, the checklist can be used to guide high-level discussions (on-site or via telephone) with management and key personnel responsible for Y2K remediation efforts.
- In the "High" category, the checklist should be used during site visit discussions with management and key personnel. In addition, the assessment should include a review of Y2K plans and supporting documentation.
- Contractors in the "Very High" category will be evaluated through actual Y2K testing. ***DCMC field offices will not perform verification testing.***

Additionally, DCAA has directed its auditors to perform certain activities regarding Y2K at both major and non-major contractor locations (98-PAS-128(R), September 14, 1998). During the assessment, the local DCAA Audit Office should be contacted to determine the results of any audits they have conducted with regard to Y2K.

In some cases (such as for site-visits at contractors in the “High” category), a multi-functional team approach may be required. When using the team approach, the team leader shall solicit the representation of all specialists deemed appropriate, including DCAA. All team evaluations shall be conducted using this checklist as a guide.

Y2K Supplier Capability Assessment Checklist

NOTICE:

This checklist is for use by government contracting/contract management personnel to guide their assessment of contractor Y2K remediation efforts

It is not a survey and shall not be mailed to contractors

SUMMARY QUESTIONS (Database input):	YES	NO
<p>1. Does the supplier indicate that they have assessed the impact of the Y2K problem? <i>Has the supplier conducted an inventory of all computer-based systems, components, external contractors (including GFP, see DCMC Tasking Memorandum No. 99-60) service providers, and hardware containing date-sensitive microchips that support the day-to-day business operations?</i></p>		
<p>2. Does the supplier believe their manufacturing or management processes are affected by the Y2K problem? <i>See Manufacturing/Operations drill-down questions.</i></p>		
<p>3. Does the supplier indicate that they are already Y2K ready? <i>See Year 2000 Readiness drill-down questions.</i></p>		
<p>4. If not, does the supplier believe that they have developed adequate plans to become ready? <i>See Management/Planning/Controlling drill-down questions.</i></p>		
<p>5. When does the supplier expect to be Y2K ready? (QTR/YYYY)</p>		
<p>6. Does the supplier believe Y2K remediation will have a material impact on its financial stability? <i>See Financial Impact drill-down questions.</i></p>		
<p>7. Has the supplier developed contingency plans? <i>See Contingency Planning drill-down questions.</i></p>		
<p>8. Is a follow-up assessment recommended? <i>Based on your assessment, should a follow-up be conducted to verify supplier Y2K efforts have been effective?</i></p>		
<p>9. From your assessment, rate the supplier's risk of Y2K related failure on a scale of 1 to 3 as follows: 1 -- High: The supplier is at "risk." 2 -- Moderate: Some aspects of the supplier's effort may be "at risk." 3 -- Low: Y2K is being address and is not expected to be a problem.</p>		

<p>DRILL-DOWN QUESTIONS:</p> <p><u>YEAR 2000 Readiness</u></p> <p>There is no standard definition of “Y2K Compliance” for supplier management or manufacturing systems (the FAR 39.002 definition only applies to all DoD purchases of information technology). However, to be Y2K ready, a system or process should be able to:</p> <p>Handle date information before, during, and after December 31, 1999, including accepting date input; providing date output; and performing calculations and comparisons. <i>The tutorial at Section V lists examples of testing criteria.</i></p> <p>Function accurately and without interruption before, during, and after January 1, 2000, without any change in operations associated with the millenium date change.</p> <p>Respond to two-digit year date input and identify the correct century. Interfacing software must make the same century assumptions when processing two-digit years.</p> <p>Recognize 2000 as a leap year?</p> <p>Recognize other key dates (e.g., 10/1/99 – start of Federal Government Fiscal Year 2000). <i>The tutorial at Section V lists some additional dates that may impact business.</i></p>	<p>NOTES:</p>
---	---------------

<p><u>MANAGEMENT/PLANNING/CONTROLLING</u></p> <p>Does the contractor have a defined and budgeted Year 2000 project that reports into senior business management?</p> <p>Has the business impact of the Year 2000 problem been assessed in terms of functions, systems, liability, business partners, customers, etc.?</p> <p>Does the contractor have clearly defined milestones and detailed plans in place for achieving these milestones?</p> <p>Do the milestones in the contractor's plan reflect their DoD contractual commitments?</p> <p>Based on the contractor's plans, are adequate skilled resources in place to deal with all dimensions of the problem in the required timeframe?</p> <p>Are Y2K projects tracking against the milestones in a timely manner to allow the contractor sufficient time to take appropriate actions?</p> <p>Does accountability for the success of Y2K remediation efforts lie directly with the contractor's business management?</p> <p>Is the contractor planning to test all business operations to assure that they will operate properly for pre- and post-Year 2000 processing?</p>	<p>NOTES:</p>
--	---------------

<p><u>MANUFACTURING/OPERATIONS</u></p> <p>Has the contractor examined its PC and server-based office automation and determined they will operate?</p> <p>Has the contractor assessed the Y2K impact on its ability to pay employees, produce financial statements, and conduct normal business not directly related to supplying customers with goods and services?</p> <p>Has the contractor assessed its ability to run its data centers?</p> <p>Has the contractor assessed the Y2K impact on its material management systems and their ability to plan and procure raw materials, manufacture, ship, and communicate shipment, etc. to customers?</p> <p>What actions has the contractor taken to assess its critical sub-contractors (i.e. surveys of subcontractors, contingency plans addressing critical subcontractors)?</p> <p>Has the contractor assessed the impact of Y2K on hardware or software (including GFP) provided by its suppliers?</p> <p>Has the contractor examined equipment on the factory floor and warehouse areas (including GFP) for devices that are date dependent such as microprocessor controlled devices?</p> <p>Has the contractor examined its HVAC, security/access, PBX, fire, and alarm system, etc.?</p> <p>Has the contractor examined its test facilities (including GFP)?</p> <p>What actions has the contractor taken regarding non-compliant hardware or software (including GFP, see DCMC Tasking Memorandum No. 99-60)?</p>	<p>NOTES:</p>
--	---------------

<p><u>FINANCIAL IMPACT</u></p> <p>Does the contractor believe the costs of Y2K remediation will have a material impact on its financial stability?</p> <p>If so, what financial actions is the contractor taking to improve/stabilize its financial position?</p>	<p>NOTES:</p>
<p><u>CONTINGENCY PLANNING</u></p> <p>Can the contractor demonstrate contingency plans for all critical business operations in case they do not function properly for pre- and post-Year2000 processing?</p> <p>Does the contractor's contingency plan address sub-tier contractors and external impact to the company?</p>	<p>NOTES:</p>

Section V

Tutorial on Y2K and Business Operations

A detailed discussion of the Y2K “fix” is provided in the pamphlet, Small Business and the Year 2000: Are You Ready to do Business in the Year 2000, published by the Manufacturing Extension Partnership (MEP). The pamphlet provides an informative, easy to understand summary of the Y2K problem. It will give field personnel the necessary background information for doing the assessments. The pamphlet is available at the MEP web-site, <http://www.mep.nist.gov/> (click on “Y2K MFG Hot Topics” icon). A hyperlink to the pamphlet is at the bottom of the MEP Hot Topics page.

Section VI

Y2K Case Studies

What Suppliers are Doing to Prevent Interruption

Several excellent case studies were published as a collection of short articles about the Y2K problem in the December 1998 issue of Inc. On Line. The articles describe what CEOs are already doing to prevent interruption of business operations. Reviewing these articles will help field personnel understand the range of approaches being used to solve the Y2K problem. The articles are available at <http://www.inc.com/incmagazine/archives/12981041.html>.

Section VII

Y2K Disclosures by Publicly Held Companies

Background: The Securities and Exchange Commission (SEC) released guidance in 1998 regarding Y2K disclosure obligations of public companies. The guidance was effective 4 August 1998, but companies with quarter ending or fiscal year ending 30 June or later are encouraged by the SEC to adhere to the requirements on the next 10-Q (quarterly report) or 10-K (annual report) filed with the SEC. SEC regulations allow a 45 day period after quarter end for filing 10-Qs, and a 90 day period after year end for filing 10-Ks.

Requirements:

- A company must provide disclosure if:
 - Its assessment of its Y2K issues is not complete, or
 - Management determines that the consequences of its Y2K issues would have a material effect on the company's business, results of operations, or financial condition, without taking into account the company's efforts to avoid those consequences.
 - *The SEC believes that Y2K issues are likely to be material for the majority of companies*
 - *The assessments of completion and of material effect include whether third parties (vendors, suppliers, etc. are compliant (if the third party has a material relationship with the company).*
- Disclosure includes information addressing:
 - The company's state of readiness;
 - The costs to address the company's Y2K issues;
 - The risks of the company's Y2K issues; and
 - The company's contingency plans.

Enforcement Power: The Securities Act of 1933 and the Securities Exchange Act of 1934 require public companies to provide full and fair disclosure to investors. There is no guarantee of the accuracy of disclosures. However, severe penalties for false or misleading information encourage company's to provide complete and accurate information.

Obtaining Y2K Disclosures

Company 10-Q and 10-K reports are public information. The reports can be obtained from a variety of sources, including internet web sites. The SEC maintains a database of reports in its “EDGAR” system at <http://www.sec.gov/>. Alternatively, “Yahoo Finance” is an excellent source (<http://quote.yahoo.com/>). Y2K disclosures in 10-Q and 10-K reports are included in the “Management Discussion and Analysis” (MD&A) section of the reports.

Guide for Reviewing SEC Disclosure Data

Securities and Exchange Commission (SEC) disclosure information refers to the information that any publicly held corporations (those that sell stock to the public) must disclose to the Government and thus to their stockholders. The SEC added Y2K information as mandatory. ***Keep in mind that this applies only to publicly traded corporations. Therefore, private companies or subsidiaries are not required to provide this information.***

First, you must determine under what name a contractor would file. If the contract is awarded to a division, or to a subsidiary, the contractor’s name would not be listed. This does not necessarily mean it is a small company. For example, Hamilton-Standard is a United Technologies Corporation so the SEC disclosure would be under UTC.

Step by step procedures:

1. Connect to EDGAR (through Yahoo finance).
2. Look for SEC disclosures under the company name as listed.
3. Look for 10Q filed most recently.
4. Page through the report to the Management Discussion and Analysis section. There is normally a paragraph entitled *Year 2000*.
5. Read through the Year 2000 section to determine the level of compliance.

If an SEC disclosure can not be found, use an Internet search engine to locate the company’s home page if available. Examine the home page to determine if the company is part of a larger corporation that may file a report. Often this higher level will have an Investor Relations area that will list the Y2K info.

If the Y2K disclosure information can be located, evaluate against the assessment checklist (see Section IV) criteria to determine adequacy. If adequate, note that on the data sheet. If inadequate or unavailable, refer the company for further assessment by phone or visit depending on assessment category.

Section VIII

Information Sources/Web-Sites

There are many helpful Internet web sites available with information on Y2K and industry efforts to address the Y2K problem. The following is a short list of some web sites that may be useful in preparing for the supplier assessments.

<http://www.sba.gov/y2k>

The Small Business Administration Y2K web site

<http://www.mep.nist.gov/>

The Manufacturing Extension Partnership

<http://www.ecrc-ctc.com>

The Electronic Commerce Resource Center

<http://www.y2k.gov>

The President's Council on Y2K

<http://www.itpolicy.gsa.gov/mks/yr2000/y2khome.htm>

U.S. Federal Gateway for Y2K Information Directories

<http://www.aia-aerospace.org/homepage/y2k.htm>

Aerospace Industries Association Y2K Home Page

<http://www.ieee.org/usab/y2k>

Institute of Electrical and Electronic Engineers Y2K Home Page

Section IX

Y2K Points of Contact DoD Joint Supplier Capability Working Group

Agency/Military Service Points of Contact

Brad Bellis, CDR	USN	703-604-9946	bellis.brad@hq.navy.mil
Nick Como	DoDIG	703-604-9215	ncomo@dodig.osd.mil
Bob Dimucci	DCAA	703-767-3282	bdimucci@hq1.dcaa.mil
Mark Gower, W/CDR	USAF	703-697-9447	gowerm@af.pentagon.mil
Robert Kratochvil	DCAA	703-767-3236	rkratochvil@hq1.dcaa.mil
David Pagano, LTC	USA	703-697-1514	pagandj@hqda.army.mil
Joe Saffron	USAMC	703-617-3567	jsaffron@hqamc.army.mil
Chris Wagner, Maj	USMC	703-695-8934	wagnrec@hqi.usmc.mil

DLA Supplier Capability Assessment Team

Mary Clarke	GC	703-767-6080	mclarke@ogc.dla.mil
Jeff Curtis	DLSC-POA	703-767-1433	jeffrey_curtis@hq.dla.mil
John Ferguson	DLSC-LS	703-767-1607	john_ferguson@hq.dla.mil
Catherine Heretick	DLSC-POA	703-767-1361	catherine_heretick@hq.dla.mil
Larry Johnson	CIR	703-767-2173	larry_johnson@hq.dla.mil
Pat Kemp	CIC	703-767-3131	pat_kemp@hq.dla.mil
Tom Lanagan	DORRA	703-767-5260	tlanagan@dscr.dla.mil
Hank Marrangoni	DESC	703-767-8632	hmarrangon@desc.dla.mil
Gloria Millen	CIC	703-767-2195	gloria_millen@hq.dla.mil
David Robertson	DCMC	703-767-3351	david_robertson@hq.dla.mil
Peter Runfola	DLSC-POA	703-767-1395	peter_runfola@hq.dla.mil
Calvin Smith	CAIW	703-767-5251	calvin_smith@hq.dla.mil
Bob Theiss	DLSC-LS	703-767-1611	robert_theiss@hq.dla.mil

DCMC Software Center

Jamileh Soudah	DCMDE	888-616-7598ext4	jsoudah@dcmde.dla.mil
----------------	-------	------------------	--